EXHIBIT 141-B

Redacted Version of

Document Sought to be Sealed

From: Richard Allan [/O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=B65F15BBE5284118A3D3619181B9F7D5]
Sent: 4/30/2019 4:28:13 AM
To: Thomas Van der Valk [tvandervalk@fb.com]; Steve Satterfield [ssatterfield@fb.com]; Erin Egan [erinegan@fb.com]; Cecilia Alvarez [ceciliaalvarez@fb.com]; Bijan Madhani [bijanm@fb.com]; Anna Van Hollen [anna@instagram.com]; Emily Sharpe [esharpe@fb.com]; Stephen Deadman [stephendeadman@fb.com]
Subject: Re: Data Portability Proposed Framework & Plan

Very interesting and good to test concepts informally in this way. I expect a lot of people will instinctively favour fully open and not like the idea of us having any kind of gatekeeper role. We will need to test them on the hard cases - eg if someone wants to transfer their data to a known privacy violator should we still stand back and do nothing to impede it? And will they stand behind us having no liability in these cases?

From: Thomas Van der Valk
Sent: Tuesday, April 30, 2019 12:12:01 PM
To: Steve Satterfield; Richard Allan; Erin Egan; Cecilia Alvarez; Bijan Madhani; Anna Van Hollen; Emily Sharpe; Stephen Deadman
Subject: Re: Data Portability Proposed Framework & Plan

Hi all,

Yesterday after the Design Jam in Paris I spoke informally with Estelle Hary from the CNIL's design team. We discussed portability, and she was quite skeptical of the idea of Facebook doing any vetting of third parties at all, primarily from a competition perspective (!). Her first response was that people should be able to take their data anywhere, and should therefore also carry the responsibility. With regard to Cambridge Analytica, she said that Facebook's main fault was that users had no idea which data was shared with Kogan in the first place.

To the suggestion that vetted Partnership Transfers could be offered as a more privacy-secure option besides the fully open transfers did not directly resonate with her. Her response was that a powerful player like Facebook would then decide which partners would be labeled secure, and which recipient parties would fall under the Fully Open Transfers (and therefore require a warning or notice). She seemed to understand that this is exactly why we'd need further guidance and regulation in this field to create an equal playing field for both third party developers and platforms, but her initial response might shed some light into how the CNIL and potential other DPAs might react to our approach.

Thanks! Thomas

From: Steve Satterfield <ssatterfield@fb.com>
Date: Thursday, April 25, 2019 at 11:38 PM
To: Richard Allan <ric@fb.com>, Erin Egan <erinegan@fb.com>, Thomas Van der Valk <tvandervalk@fb.com>, Cecilia Alvarez <ceciliaalvarez@fb.com>, Bijan Madhani <bijanm@fb.com>, Anna Van Hollen <anna@instagram.com>, Emily Sharpe <esharpe@fb.com>, Stephen Deadman <stephendeadman@fb.com>
Subject: Re: Data Portability Proposed Framework & Plan

Thanks, Richard. This is awesome and really helpful. Bijan and I will work up a new version of the framework.

Steve Satterfield
Facebook Public Policy
650-465-9473

From: Richard Allan
Sent: Thursday, April 25, 2019 10:13:38 AM
To: Erin Egan; Thomas Van der Valk; Cecilia Alvarez; Bijan Madhani; Anna Van Hollen; Steve Satterfield; Emily Sharpe; Richard Allan; Stephen Deadman
Subject: Re: Data Portability Proposed Framework & Plan

I had some thoughts after the call yesterday and took some time to throw them into a document today. This is attached and pasted below. Feel free to use or discard as you see fit! It's not a highly polished doc but I wanted to get these ideas down while they were top of mind in case this is helpful. R.

Some notes from the discussion yesterday.

Types of Data

A useful way to categorise data is to look at who can exercise the functions of a data controller for different classes of data.

Own Data. For data that I upload and share with a service, I have the controller functions. I decide when to upload the data, I can edit it, and I decide when to delete it. It is these powers that make it fully "my personal data".

Shared Data. For data that is shared with me by other users, they have the controller functions. They decide when to upload the data, they can edit it, and they decide when to delete it. This is what makes it "their personal data" rather than mine.

Platform Data. For data that is inferred or generated by the platform, the platform has the controller functions. The platform decides what data to generate when and has the power to delete this data. This is the platform's data.

To complicate matters, in each case ownership does not exclude others from having an interest in and rights over the data.

Under 1, there will be other people who have an interest in data like contact information and photos that I "own".

Under 2, I will have an interest in the data "owned" by other people where it contains personal information about me.

Under 3, I will have an interest in the data "owned" by the platform to the extent that it contains personal information about me or is inferred from my personal data.

In defining the scope of a "right" to data portability we need to consider the interests related to each of these classes.

Class 1 is what is top of mind for most people when talking about portability. It is assumed that this class of data can be made portable in its entirety. The major open question is how to respect the interests of other people in this data.

The simplest solution would be to place this responsibility fully on the data "owner". The owner would be asked to assure themselves that any 3rd parties are content with the data transfer and would be fully liable if there were any complaints about the owner making the transfer.

At the other end of the spectrum, platforms could be required to seek consent from 3rd parties for any transfer that includes data referencing them. As a practical matter, this would be extremely challenging. A platform would not necessarily know who is in photos and therefore needs to be consulted, or the terms under which contact details have been shared between individuals. In many cases the platform will have no relationship with a 3rd party and so the act of seeking consent could itself be seen as intrusive, eg if this involved platforms sending emails to non-users to ask consent for a transfer.

If we are to meet people's expectations in terms of the right to portability, the correct solution here is likely to be the model where the responsibility does fully sit with the data "owner" and platforms are not required to place additional controls in place. 3rd parties referenced in the owner's data will still be able to exercise their rights but must do so against the owner rather than against the platform.

Class 2 is the most sensitive type of data as we have seen with the debate triggered by Cambridge Analytica.

The simplest solution here is to exclude this class of data fully from the right to data portability. The other data owner would have the full portability rights and you would acquire no such rights just by virtue of the data being shared with you. This requires the adoption of a definition of "your" personal data that excludes that where you have an interest but are not the owner.

There are also some types of sharing that raise special questions. Where someone has shared a social media post with friends, it seems obvious that they continue to be the "owner" as distinct from those who can access the post.

Where an email or message is sent between two people it will typically exist in accounts operated by each party. It is arguable that this data has been transferred between the parties and they now each control their copy of it equally rather than there being one controller. Accepting this logic then content that has been sent to someone and now sits in some form of inbox falls into category 1 - it is personal data they now "own" and control as a recipient while the sender owns and controls their copy of the same data.

It is possible to imagine messaging system models that work more on the post sharing model, ie the commitment is that only the sender owns a message with the recipient simply being given permission to view it. For the purposes of data portability it is important that everyone knows which model is in operation for each service - are they merely sharing a message or are they granting ownership of a copy of the message to the recipient - and can moderate their behaviour accordingly.

Class 3 is something that many advocates for data portability are keen to see included. A key motivation for this is that they want to see increased transparency around how platforms are using personal data and "algorithms". Transparency does not strictly require this data to be made portable as long as it is visible somewhere.

The other motivation is that of creating more competition between platforms and this does require portability, ie the assumption is that there will be value for platforms receiving data in having access to the data generated by the sending platform.

The open questions here largely revolve around balancing the rights of the user with those of the platform rather than a tension between the interests two or more different users as in classes 1 and 2. There are other user rights that require consideration of similar issues, notably subject access rights and rights in relation to automated data processing. It would make sense for there to be alignment here so that a common definition is used for the class 3 data that platforms must include for the purposes of responding to a subject access request and offering data portability with a subset of this being the data they must provide to meet obligations in relation to automated data processing.

Types of Portability

There will normally be three parties directly involved in the kinds of data transfers we are considering under the banner of social media data portability. These are the requesting user, the hosting platform and the recipient.

It is essential to understand what responsibilities fall on each party and these may vary according to the conditions under which the transfer takes place. We can break these down into three broad categories.

Fully Open Transfer. In this model the requesting user can send their data to any recipient without any controls or limitations being imposed by the hosting platform. This model only works if the user is deemed to be solely responsible

for the transfer as the platform has no power to condition or prevent a transfer. There might be scope for platforms to provide some kind of guidance to users around the transfer but it is important that this guidance is not seen as creating liability for the platform over a transfer it does not control.

This is functionally equivalent to moving data from your device directly to a new service. An existing installed application has no ability to control when you send your local data to a new application or liability for this. In this case, there is a step of extracting data from the existing application that takes place before the transfer to the new one. This could happen with the data physically moving through the device as a staging post or the data could be transferred directly between the applications under the same conceptual model as long as full control of the transfer is in the hands of the requesting user.

Conditioned Transfer. In this model the requesting user can send their data to any recipient that has met certain conditions required by the platform. The requesting user has the primary responsibility as the instigator of the transfer but there may also be a secondary responsibility on the platform to ensure that recipients are meeting any specified conditions.

When the user asks for this kind of transfer the Platform will check that the recipient meets whatever criteria have been set and only perform the transfer if all is in order. This requires the Platform to stand between the requesting user and recipient at the time of transfer. The conditions under this model will only be relevant at transfer time, for example a check that the recipient has a privacy policy in place at that moment, and the platform will be free of further liability after the transfer has taken place.

Partnership Transfer. In this model the requesting user is sending their data to a recipient who has an ongoing contractual relationship with the platform including provisions on how they should treat data. Responsibility for data will continue to be shared between the platform and the recipient.

There may be a series of requirements specified in the partnership agreement about the uses to which data can be put, security measures, deletion provisions etc. If will be for the recipient to meet these requirements or risk losing both data protection enforcement and contractual sanctions. It will be on platforms to monitor and enforce against those with whom they have agreements and they could face sanctions if they make errors either by failing to maintain standards or by treating partners unfairly.

It is important to note that these models are not mutually exclusive. It is possible that all three models could be in operation between a platform and the same recipient.

People can always use the Fully Open Transfer model to take their data and move it to another service without involving the platform at all.

If the recipient service has signed up for a Conditioned Transfer model like the Data Transfer Project then the user will be able to use this as an alternative way to move their data.

The underlying technology may even be the same for both methods but there would be different processes for authorising and putting the transfer into effect.

The recipient service may also have an agreement with the platform that offers a deeper integration with ongoing regular transfers of data under the Partnership Model.

We can imagine this as a pyramid where all services will need to offer the Fully Open base layer and then they will have choices about whether to offer their users additional functionality in the other two Conditioned and Partnership layers and how extensive that offer should be.

A Workable Model

These are issues where we are trying to balance the rights of different parties. There is no single right answer but people will rather take different views of the trade-offs and where we should land. We should consult widely on all possible models but this can be informed by how we think the balances will play out.

A baseline standard for a "right" to data portability would be to offer a Fully Open Transfer capability only for Own Data. This can be met today by the DYI tool that Facebook provides (which also includes elements of Shared Data and Platform Data).

If we see this as a genuine right, akin to a property right, then it is hard to see a scenario in which this Fully Open model will not be a requirement. It will be important to get clarity on the design of the transfer process and any guidance that can be offered by platforms so that their solutions are considered Fully Open and do not confer liability on the platform.

It is in the interests of privacy that platforms should also be encouraged to develop ecosystems for Conditioned Transfers. These will allow for appropriate controls to be put in place that give additional assurances to users in relation to the privacy of their data. [redacted] is a good example of how such an ecosystem might be built.

It is important to recognise that this is not a substitute for the Fully Open Model but a complement to it. Concerns may be raised about differential treatment if there is additional functionality available for those eligible for Conditioned Transfers but as long as the conditions being applied are fair and reasonable it would be perverse to rule out a model which may incentivise good privacy practices.

In practical terms, the difference between these two models would be largely in terms of ease of use. A Fully Open Transfer will require specific steps to confirm that requesting user fully understands the terms of the transfer and it may require more manual processes. A Conditioned Transfer may be smoother because a certain amount of due diligence was done before access was granted to that transfer method.

[redacted] in some senses beyond the scope of the "right" to data portability. It is not about an individual freely exercising their rights to move their data but rather an ongoing [redacted] that involves the transfer of user data. It creates a framework within in which more types of data may be transferred, for example it may be possible to get user consents to transfer Shared Data or to offer enhanced Platform Data within these [redacted]

It is essential that there is real clarity around which model is being used and that this is apparent to all interested parties. A challenge with previous iterations of Platform has been a lack of clarity about which model is in play. Language used to describe it has had elements of both the Fully Open Model - it is users who make all the decisions about when to share their data - through to the [redacted] - we impose meaningful conditions on developers.